Current Threat Environment

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Mark Sherman, PhD
Technical Director, CERT
mssherman@sei.cmu.edu

29-Aug-2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
29 AUG 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Current Threat Environment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Sherman /Mark S.	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**16**	

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

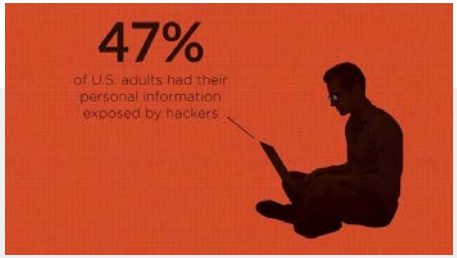
DM-0001785

Current Threat Environment

- Usual view of threat environment
- Looking backwards from today's threats
- Looking forwards to future threats
- The need for prevention is pressing

Mark Sherman
Cyber Security Foundations Research

Usual view of threat environment



Sources: Poneman Institute, CNNMoney study, May 28, 2014; McAfee Quarterly Threat Report, June 2014; Wall Street Journal, Feb 26, 2014

retailcustomerexperience.com - 5_lessons_learned_from_recent_retail_data_breaches.pdf

Mark Sherman
Cyber Security Foundations Research

Looking backwards from today's threats

92% of the 100,000 incidents from the last 10 years can be described by 9 basic patterns

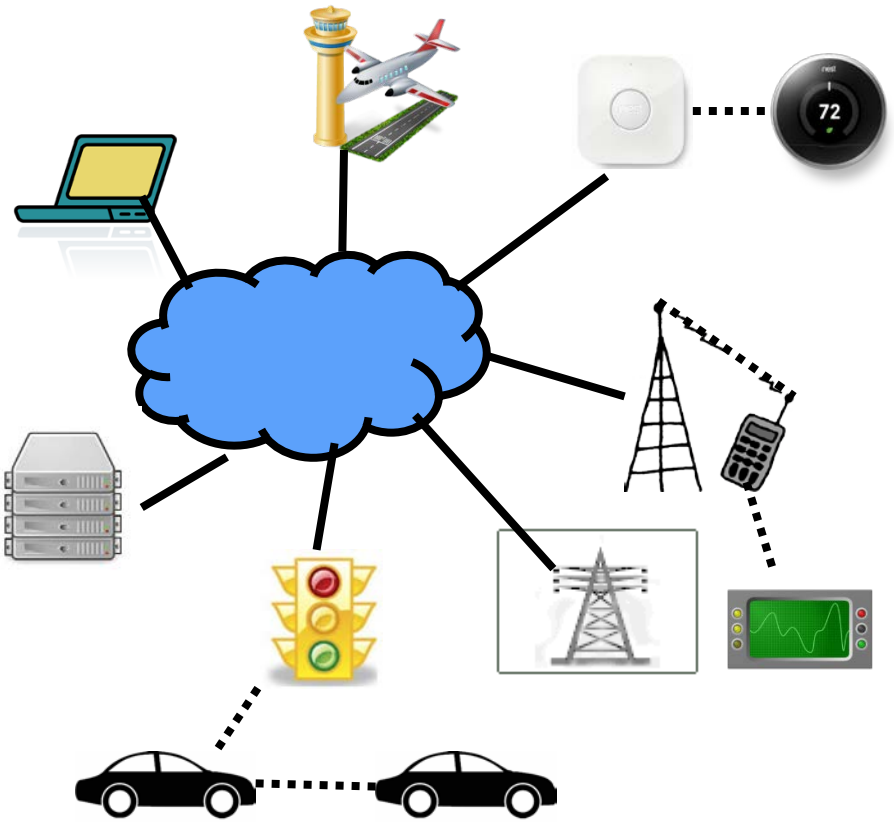
- Insider misuse
- DOS attacks
- Cyber-espionage
- Crimeware
- Web app attacks
- Physical theft and loss
- Payment card skimmers
- Point-of-sale intrusions
- Miscellaneous errors

Mark Sherman
Cyber Security Foundations Research

Looking forward to future threats

- Technology
- Evolving role of people in cyber security
- Learning from data: measurements, metrics, analysis

Cyber threats track evolution of technology



- Software is the new hardware
- Covering the next last mile
- Expanding endpoints

Mark Sherman
Cyber Security Foundations Research

Software is the new hardware

IT moving from specialized hardware to software, virtualized as

- Memory
- Storage
- Servers
- Switches
- Networks

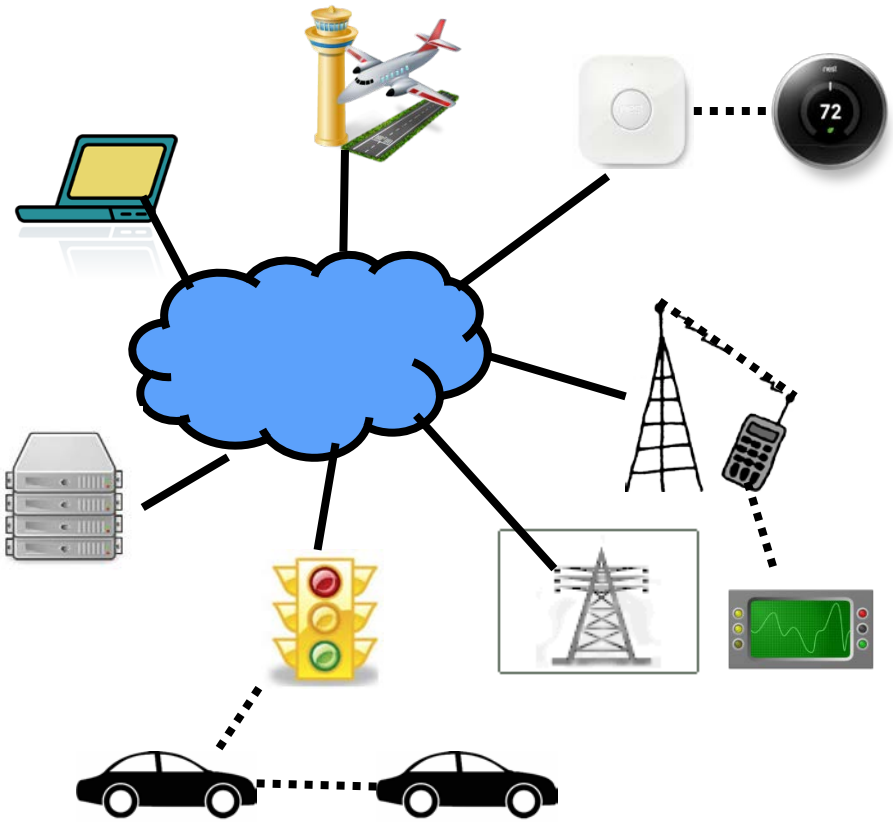
Cyber-physical systems (CPS) evolving to a computer with interesting peripherals

- Airplane function in software moved from 8% to 80% since 1960
- Software defined radios drive communication
- Television evolved to digital signal processors

- Hardware security needs software analogs
- New programming models need secure coding guidelines
- Guard against side channel attacks enabled by virtualization

Mark Sherman
Cyber Security Foundations Research

Covering the next last mile – securing the border and end points



The last mile has expanded to

- Cellular
  - Main processor
  - Base band processor
  - Secure element (SIM)
- Industrial and home automation
  - SCADA
  - Bluetooth
  - Zigbee
- Automotive
  - Intravehicular: more than 50 networked processors
  - Vehicle to infrastructure (V2I): congestion management, emergency services, law enforcement
  - Vehicle to vehicle (V2): safety, efficiency
- Aviation
  - Fly by wire
  - Next Gen air traffic control
- Smart grid
- Embedded medical devices

Evolving role of people in cyber security

Analysts: Soaring need for cyber analysts

- Bureau of Labor Statistics projects information security analyst jobs to increase by 20% or more through 2018
- Need validated measurement and testing of needed skills, at individual and team level

Optimizing analyst effectiveness: Automation assists analysts

- What can be automated and what left to the analyst
- Trade off between training and application

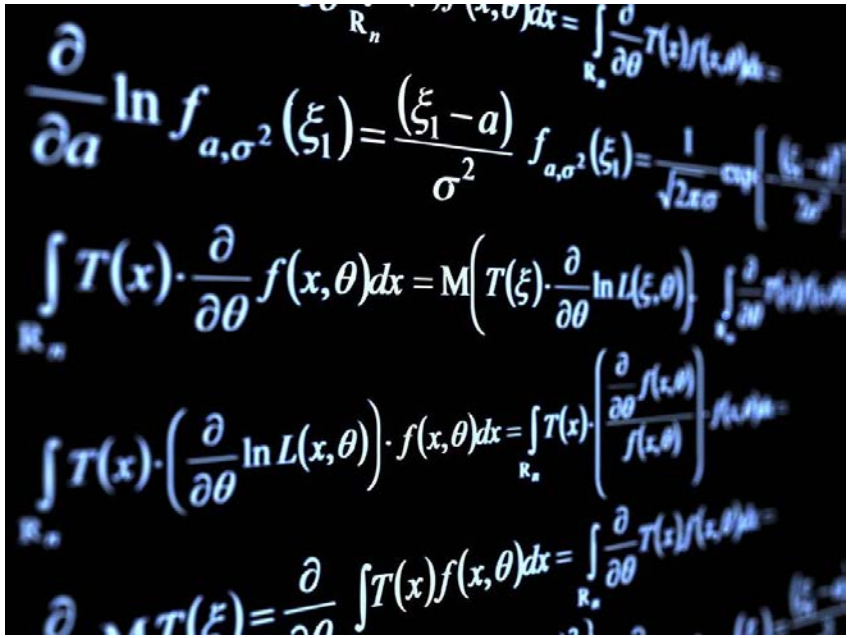
Developers: Development becoming assembly over creation

- At least 75% of organizations rely on open source as the foundation of their applications
- Weak or absent security tracking in the software supply chain

Adversaries: Culture role in cyber security

- Cultural influences on development and attack behavior

Learning from data: measurements, metrics, analysis



Biggest challenges

- **Determining leading indicators**
- **Reducing false positives**

Need to extract information from data from across the software lifecycle

Applying techniques across disciplines including

- Metric and model definition
- Social and psychological experimentation
- Machine learning
- Statistical modeling

Applications to

- Real-time analysis
- Retrospective insight

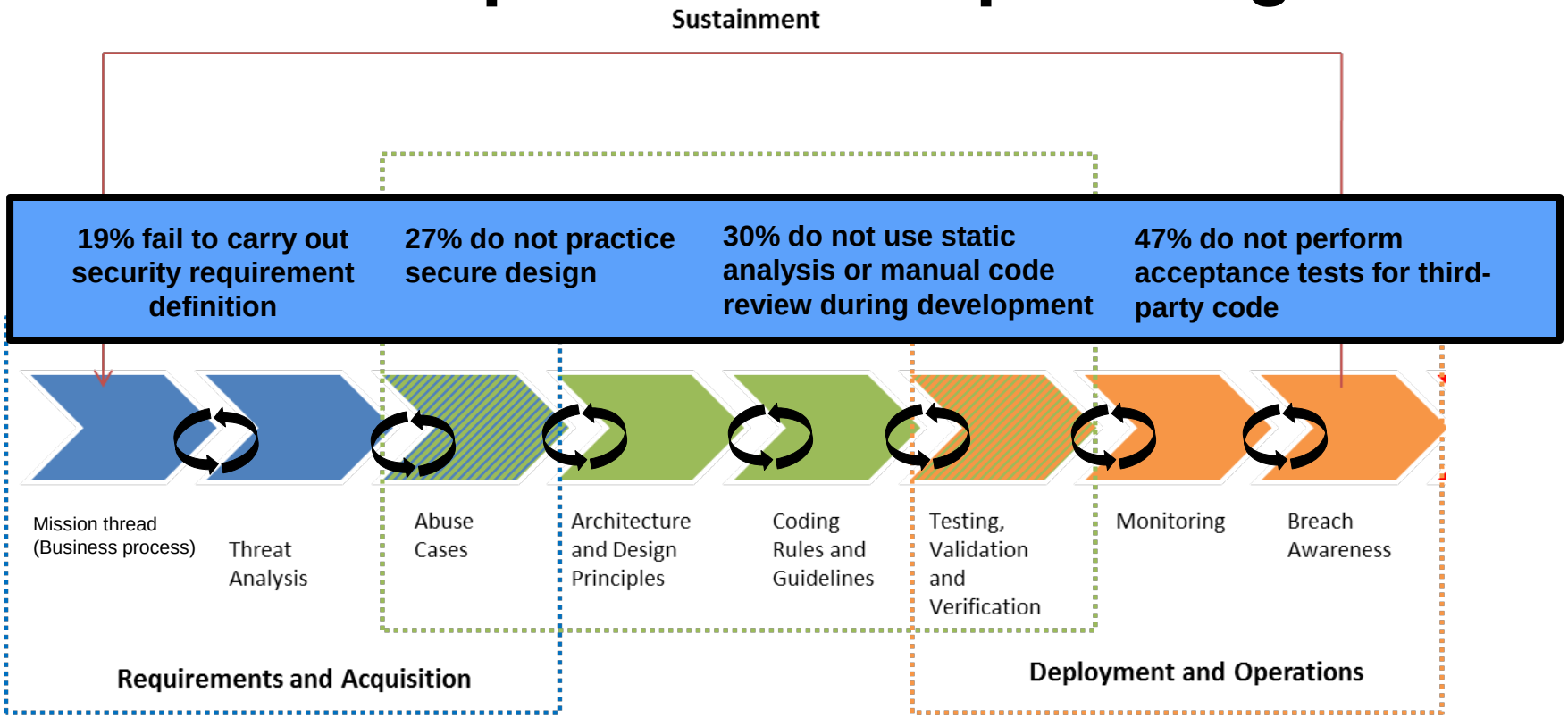
An ounce of prevention is worth a pound of cure

> “We wouldn't have to spend so much time, money, and effort on network security if we didn't have such bad software security.”

Bruce Schneier in Viega and McGraw,
“Building Secure Software,” 2001

Mark Sherman
Cyber Security Foundations Research

The need for prevention is pressing



More than 81% do not coordinate their security practices in various stages of the development life cycle.

Source: Forrester Consulting, “State of Application Security,” January 2011

Security by default

Contact Information

Mark Sherman

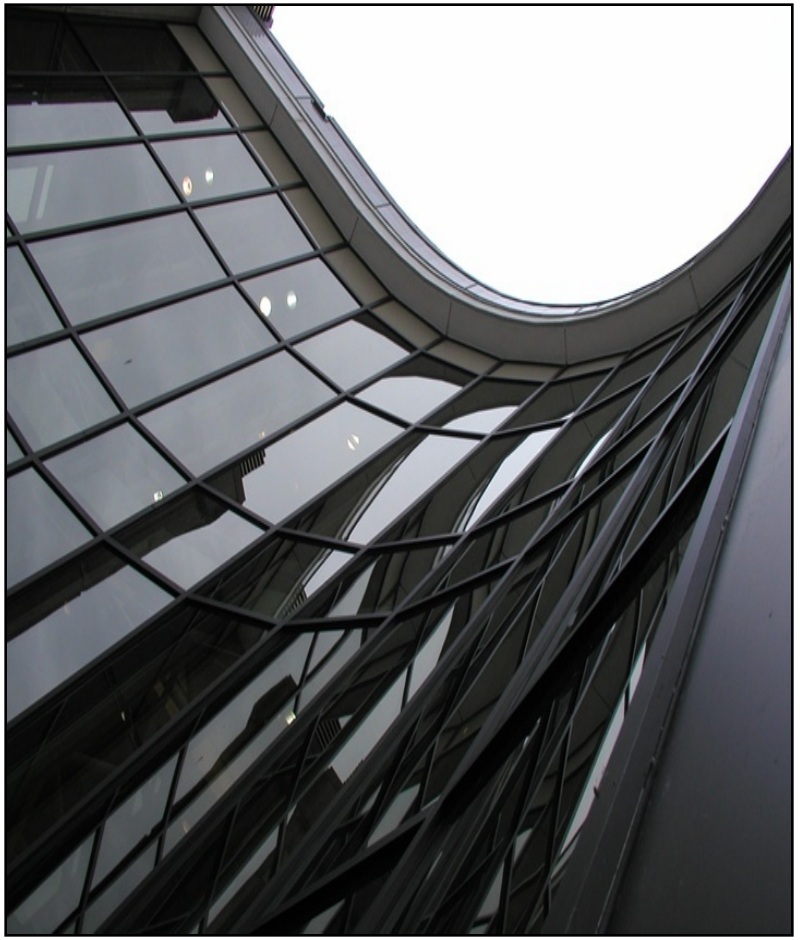
(412) 268-9223

mssherman@sei.cmu.edu

Web Resources (CERT/SEI)

http://www.cert.org/

http://www.sei.cmu.edu/



Software Engineering Institute | Carnegie Mellon University